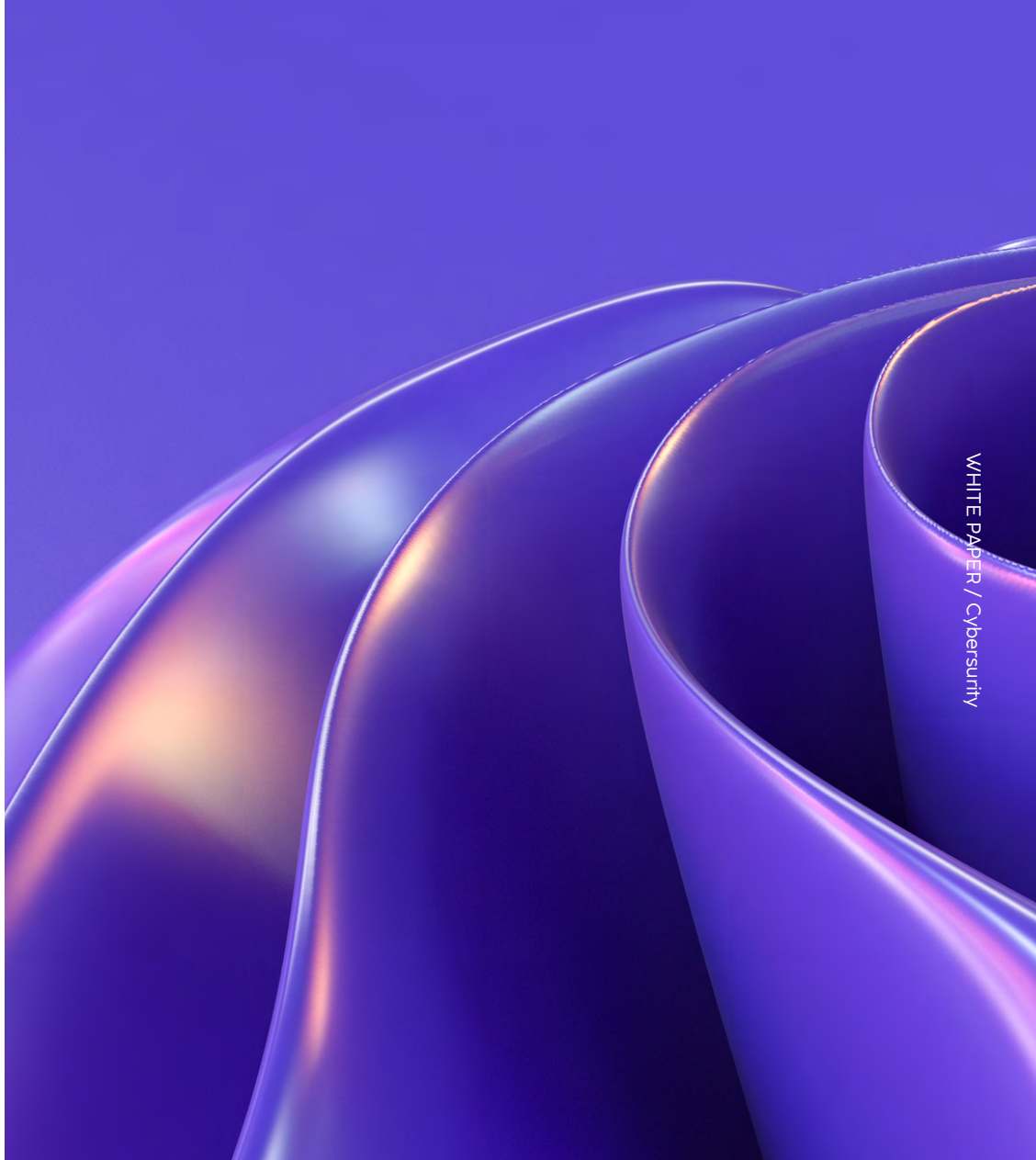
WHITE PAPER

# Cybersecurity





# Autori

**Roberto Pignani**
Cybersecurity Director

**ENGINEERING**
roberto.pignani@eng.it

**Emanuele Cacciatore**
Offering, Innovation & Deal Management Director

**ENGINEERING**
emanuele.cacciatore@eng.it

**Paolo Roccetti**
Head of cybersecurity Research Unit
Engineering R&D

**ENGINEERING**
paolo.roccetti@eng.it

# Sommario



# 01 Un business sicuro è un business che può crescere

**Il mondo in cui viviamo sta evolvendo rapidamente**: l'innovazione sta portando miglioramenti a una velocità senza precedenti nel nostro modo di vivere e lavorare. Tuttavia, nella misura in cui la tecnologia semplifica la vita, aumenta anche la vulnerabilità agli attacchi informatici.

La **Digital Transformation** impone alle aziende due imperativi fondamentali e divergenti:

- **abilitare** e far crescere il business, implementando servizi on line che interagiscano in modo sicuro con i dipendenti, i clienti e i partner, e rendendo la propria struttura più efficiente e agile così da rispondere rapidamente alle nuove esigenze del mercato
- **proteggere** il business da violazioni, dati e accessi impropri, grazie a controlli in grado di salvaguardare i dati ovunque essi si trovino (dispositivi mobile, portatili, data center e Cloud)

La **Cybersecurity** è la raccolta strutturata di tecnologie, competenze e processi, in grado di prevenire, rilevare e reagire efficacemente contro gli attacchi alle persone, ai dati, alle applicazioni e alle infrastrutture.

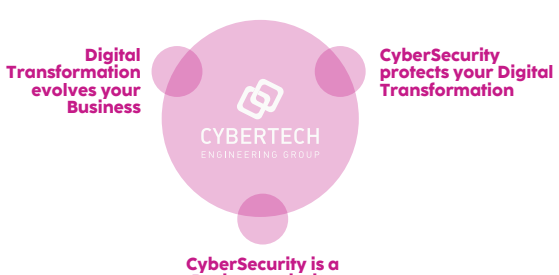
Alla crescita esponenziale della quantità e del valore dei dati (codice, testo, immagini, infografica, video, segnali), corrisponde in modo diretto l'importanza dell'adozione della Cybersecurity.

Trascurare alcuni elementi fondamentali, come il fatto di garantire una continua protezione informatica e fornire la consapevolezza della sicurezza informatica ai dipendenti, può generare dei costi importanti a lungo termine. Ecco perché la protezione informatica dovrebbe diventare un "**must-have**", non un "nice to have" nel processo decisionale.

Questo cambio di mentalità richiede la valorizzazione della cultura della sicurezza informatica in ogni aspetto del business, sfruttando un mix di esperienze, competenze e giuste tecnologie per garantire una trasformazione digitale sicura e controllata.

Essendo impossibile raggiungere un grado di sicurezza totale, è dunque necessario definire una strategia di cybersecurity, selezionando e bilanciando dove e come concentrare gli interventi, utilizzando un approccio basato sulla priorità di mitigazione del rischio.

In questo scenario, la Cybersecurity non è soltanto un argomento di business, ma è un requisito essenziale la crescita e l'evoluzione di ogni azienda.



# 02 La moderna Cybersecurity va ben oltre la difesa passiva

Nel contesto odierno, caratterizzato da crescenti e mutevoli minacce informatiche ad aziende, enti pubblici e gestori di infrastrutture critiche, la Cybersecurity è al centro delle agende delle realtà e dei vari ruoli che sono coinvolti a livello sia strategico che operativo.

Gli attacchi informatici spesso comportano degli impatti sostanziali per il business legati all'interruzione dell'attività, alla perdita finanziaria e ai danni reputazionali.

In un ecosistema digitale in rapida evoluzione, ci sarà sempre di più la necessità di anticipare e affrontare le sfide della sicurezza informatica per stare al passo con i tempi, con un focus sul rafforzamento della resilienza (cyber resilience).

Le priorità ed i driver della Cybersecurity che popolano le agende di questi stakeholders includono molteplici temi, tra cui:

## Bloccare gli attacchi cyber

Proteggersi dal rischio di malware avanzato, attacchi mirati, persistenti e silenti, e minacce di Cybersecurity provenienti dall'interno.

## Indirizzare il problema della carenza di competenze

Assicurare Security Operation efficaci e 24x7 nonostante l'insufficienza di competenza, sia interna all'azienda sia sul mercato.

## Gestire la complessità tecnologica in continua evoluzione

Saper gestire molteplici prodotti che indirizzano ciascuno un dominio della sicurezza, con limitata capacità di integrazione ed in continuo aggiornamento.

## Governare la crescita delle Identità digitali

Garantire un controllo di tipo zero trust, continuo e selettivo degli accessi a sistemi, dati ed applicazioni in un contesto in cui le identità digitali sono disperse, in volume, varietà e disseminazione.

## Mettere in sicurezza i dati critici

Proteggere la proprietà intellettuale nelle varie fasi di discovery, classificazione, attribuzione del rischio di perdita o manipolazione indebita del dato, hardening dei repository dei dati, controllo degli accessi alle informazioni, e tutto questo sia per dati strutturati che non strutturati.

## Proteggere le infrastrutture critiche

Partire dall'identificazione degli asset critici, peculiari per ogni contesto aziendale, e prioritizzare gli investimenti in logica di risk management.

## Proteggere il perimetro esteso

Assicurare la protezione, in una logica Zero-Trust, di dati e applicazioni ormai distribuite nel Multi-cloud Ibrido, negli ecosistemi B2B, B2E, B2C, incluso l'IoT.

## Creare cultura cyber diffusa e stare al passo con le conformità normative

Aumentare l'awareness sulla postura digitale della sicurezza (Cyber Posture) dell'intero sistema e fare leva sui mandati operativi ed adempire alla prescrizioni generali e di settore (GDPR, PSD2, PCI/DSS, NIS2, DORA, ...).

## La Cybersecurity riduce i rischi e aumenta la tua consapevolezza

**$9,2 Trilioni**

**IMPATTO GLOBALE DEI DANNI DOVUTI AL CYBERCRIME NEL 2024**

**$4,45 mln**
COSTO MEDIO DI UNA VIOLAZIONE DEI DATI IN 2023 ($3.86 M in Italia)

**+25 mld**
DISPOSITIVI IOT INSTALLATI A LIVELLO GLOBALE ENTRO IL 2030

**277**
MEDIA GIORNI PER IDENTIFICARE E CONTENERE UNA

**80%**
LE AZIENDE CHE HANNO SUBITO UNA O PIÙ VIOLAZIONI DEI DATI NEL 2023

**82%**
DELLE VIOLAZIONI ESAMINATE SONO BASATE SUL CLOUD (PUBBLICO O PRIVATO)

**+3,5 mln**
POSTI LAVORATIVI NON COPERTI STIMATI NEL CAMPO DELLA CYBERSECURITY

## Top 3 Impatti di Business

**Interruzione del servizio**

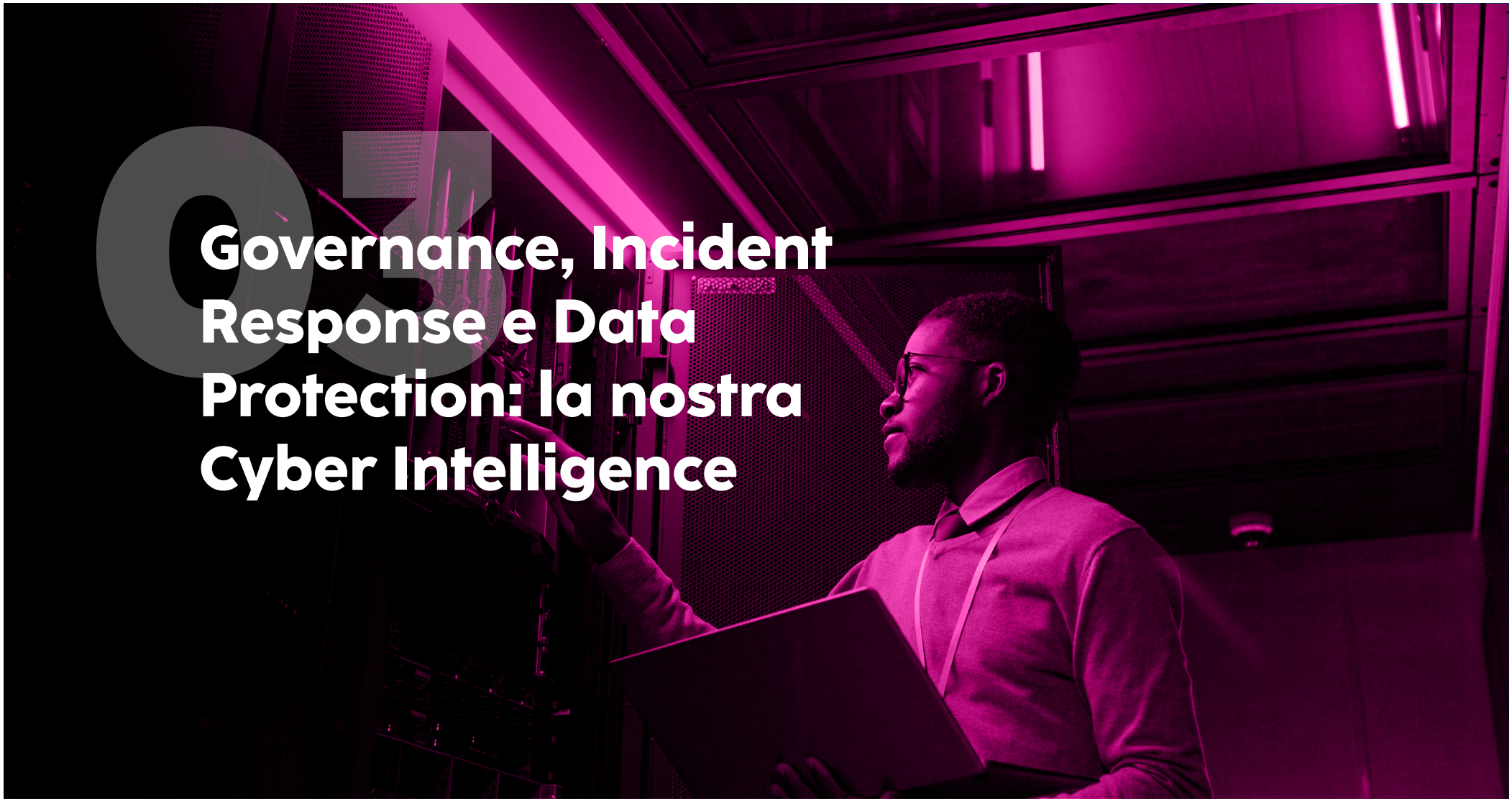
**Perdite Economiche**

**Danno Reputazionale**

## Le sfide principali derivano da:

Malware, Ransomware, Configurazioni errate, Phishing/Social Engineering, Furto di identità e Attacchi interni.

I dati visualizzati rappresentano la nostra elaborazione di dati provenienti da più fonti.



# 03

# Governance, Incident Response e Data Protection: la nostra Cyber Intelligence

# Cybertech Engineering's Cybersecurity Company

Engineering garantisce una sicurezza informatica costante. Chi sceglie il nostro approccio alla Cybersecurity potrà concentrarsi sulla crescita del proprio business, perché avrà al proprio fianco un partner in grado di formare i dipendenti, controllare le reti, salvaguardare i dati e prevenire le minacce informatiche prima che abbiano un impatto per l'azienda.

I nostri continui investimenti in persone e ricerca assicurano inoltre che il nostro approccio alla sicurezza evolva costantemente e in maniera allineata alla complessità del nostro mondo.

**Abbiamo la visione, le risorse e l'esperienza per proteggere la tua organizzazione mentre intraprende il suo digital journey.**

## Abilitiamo una Digital Transformation sicura per la tua organizzazione

Proteggiamo dati, reti e infrastrutture, e garantendo uno spazio digitale sicuro per dipendenti, clienti e partner.

**Siamo membri di European Organization for Security (EOS) e di European Cyber Security Organization (ECSO)**

**300+**
SPECIALISTI IN CYBERSECURITY

**550+**
CERTIFICAZIONI INDIVIDUALI

**450**
CLIENTI

**20+**
PAESI DOVE ABBIAMO CLIENTI

**500**
SECURITY ALERTS GESTITI IN MEDIA OGNI GIORNO

**+7M€**
VOLUME ECONOMICO DEI PROGETTI ATTIVI DI R&I

**1**
SOC CERTIFICATO ISO27001/2017

**2**
SOC CONTROL ROOMS: ROMA, BOLOGNA

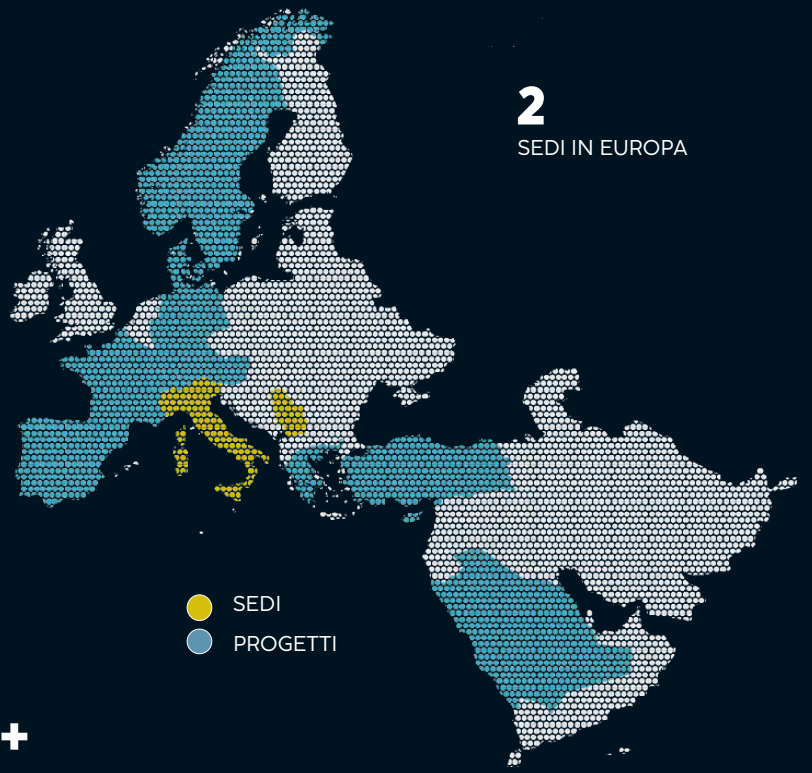
**50+**
0-DAY (WITHOUT CVE OR IN BUG BOUNTY PROGRAM)

**35+**
OFFICIAL CVE RELEASES

**3**
DATA CENTER TIER IV, AGID, ISO27001/ 2013, TIA-942

**1**
LABORATORIO DI PROVA PER LA VALUTAZIONE DELLA SICUREZZA INFORMATICA ISO17025

**30+**
ETHICAL HACKER




**2**
SEDI IN EUROPA

Per una **strategia di investimento** completa ed efficace, è fondamentale valorizzare persone, processi e tecnologie. Ma come fare in modo sostenibile? L'approccio al **risk management** è la risposta:

- Identificare la superficie di attacco e gli asset chiave per le operazioni aziendali;
- Contestualizzare il rischio e prioritizzare le azioni di remediation in base alle tipologie di attacchi avvenuti nel settore;
- Arricchire il portfolio di difesa testando le risposte ad eventi inaspettati;
- Rimediare ai punti deboli identificati, sia quelli tecnologici che quelli di processo;
- Valutare e misurare in ottica di continuous improvement, le azioni necessarie per supportare l' evoluzione dell'impresa.

Per affrontare le sfide della Cybersecurity, è necessario un approccio olistico ed una sicurezza "in-depth" multi livello, che integri soluzioni verticali e trasversali per impattare device, identità, dati, infrastrutture tecnologiche, workload e servizi applicativi distribuiti nel Cloud, nonché per orchestrare tecnologie, processi e competenze secondo gli standard di riferimento e le moderne metodologie e buone pratiche di mercato.

L'obiettivo è diventare adattivi e resilienti al rischio cyber, guardando alla sicurezza come **prevenzione proattiva, rilevamento anticipato, rapida risposta, e advanced security analytics.** La trasformazione digitale richiede dunque un nuovo approccio alla Cybersecurity, multidimensionale e trasversale, in grado di mettere in campo competenze basate su tecnologie avanzate di rilevamento delle minacce e di protezione efficace.

Ogni approccio deve integrarsi alle conoscenze e ai processi già presenti in azienda, per garantire una difesa completamente allineata alle altre attività.

Per agevolare un'adeguata comprensione e mitigazione del rischio-cyber, consentendo l'applicazione di contromisure in una logica di riduzione e controllo del rischio guidato dalle priorità di business sia in ambito organizzativo che tecnologico abbiamo quindi disegnato un approccio alla Cybersecurity basato su **tre pilastri**:

Pillars

## Governo delle identità digitali

**Per controllare dinamicamente ed in una logica "Zero Trust" gli accessi ad applicazioni e dati fondamentali, anticipando la compliance, mantenendo nel contempo allineate le prospettive dell'audit, dell'IT, e delle Line of business (LOB).**

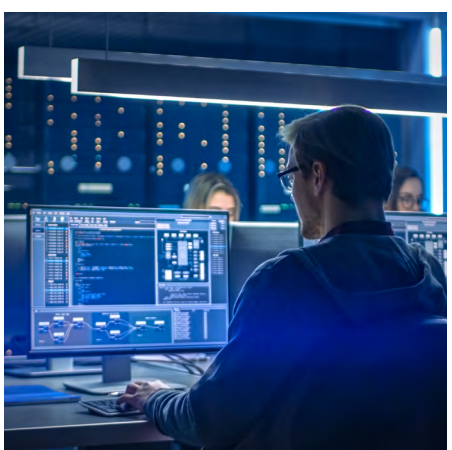
Il moderno paradigma di governo delle identità digitali è basato su una logica Zero Trust, con un sistema di controllo ed enforcement centralizzato in grado di autenticare, autorizzare e connettere (con verifiche continue e granulari) identità digitali ormai disperse tra utenti (sia essi interni all'azienda, inclusi gli accessi da amministratore, sia quelli esterni di clienti e terze parti), device connessi IoT ed API, verso applicazioni e servizi distribuiti tra on-premise e – sempre più – nel Cloud.

## Blocco degli attacchi-cyber

**Per intercettare e fermare le minacce avanzate, persistenti e interne, facendo leva su Security Operations con caratteristiche avanzate di analisi dei dati e di automazione**.

Insieme ad un'adeguata capacità di orchestrazione di tecnologie, processi e competenze di Cybersecurity, è possibile garantire un contrasto ed una risposta efficace ed ordinata agli incidenti di sicurezza. Un perimetro di sicurezza “fluido” e in continua evoluzione richiede una difesa multidimensionale, con presidi progressivi in grado di intercettare le minacce lungo la "kill chain".

È qui che entra in gioco l’**Intelligence and Automation Driven Security Operation Center (IASOC)**, che fornisce un sistema centralizzato, guidato dall’Intelligenza Artificiale, ed ad alta intensità di Automazione dei Processi, che integri ed orchestri i diversi livelli e presidi di sicurezza, consolidando in una vista unificata le allerte qualificate, il rilevamento degli incidenti, e le azioni di reazione e recupero.

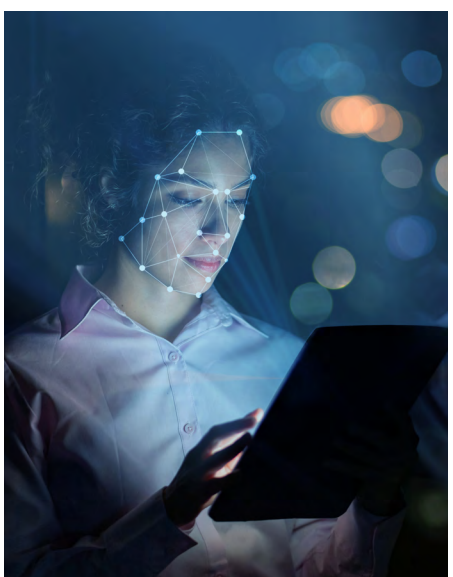


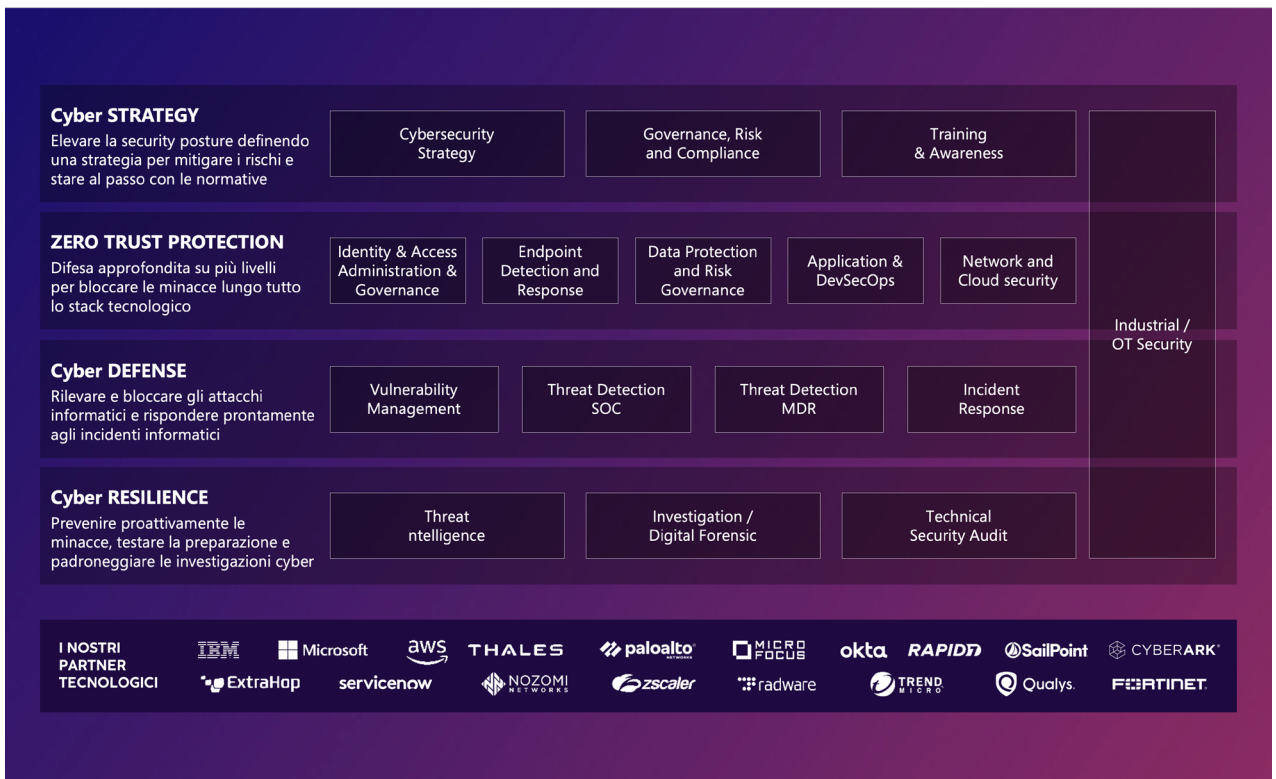
## Salvaguardia dei dati

**Per controllare il rischio di accesso indebito e manipolazione dei dati, proteggerne il brand e abilitarne il business digitale in tutto l’ecosistema aziendale B2E, B2C, B2B, dei workload nel cloud ibrido e degli asset più importanti di un’organizzazione**.

Per un’azienda che gestisce il business digitale i dati sono una delle sue risorse più importanti.

Oggi, però, la loro sicurezza è messa alla prova dal fatto che sempre più informazioni, sia strutturate sia in formato non strutturato, vengono modificate, condivise, archiviate localmente o nel Cloud, e con processi che, se mal gestiti, possono provocare vulnerabilità.
Le nuove normative sulla privacy, inoltre, stanno creando requisiti sempre più stringenti su come gestire i dati, specialmente se relativi ad individui.






Infine, grazie ad elevati investimenti in tecnologie a risorse, abbiamo disegnato un portfolio di servizi completo, modulare e altamente flessibile, che utilizza le soluzioni best-of-breed nel mercato.

04

# Soluzioni integrate multilivello offrono sicurezza a tutta l'organizzazione

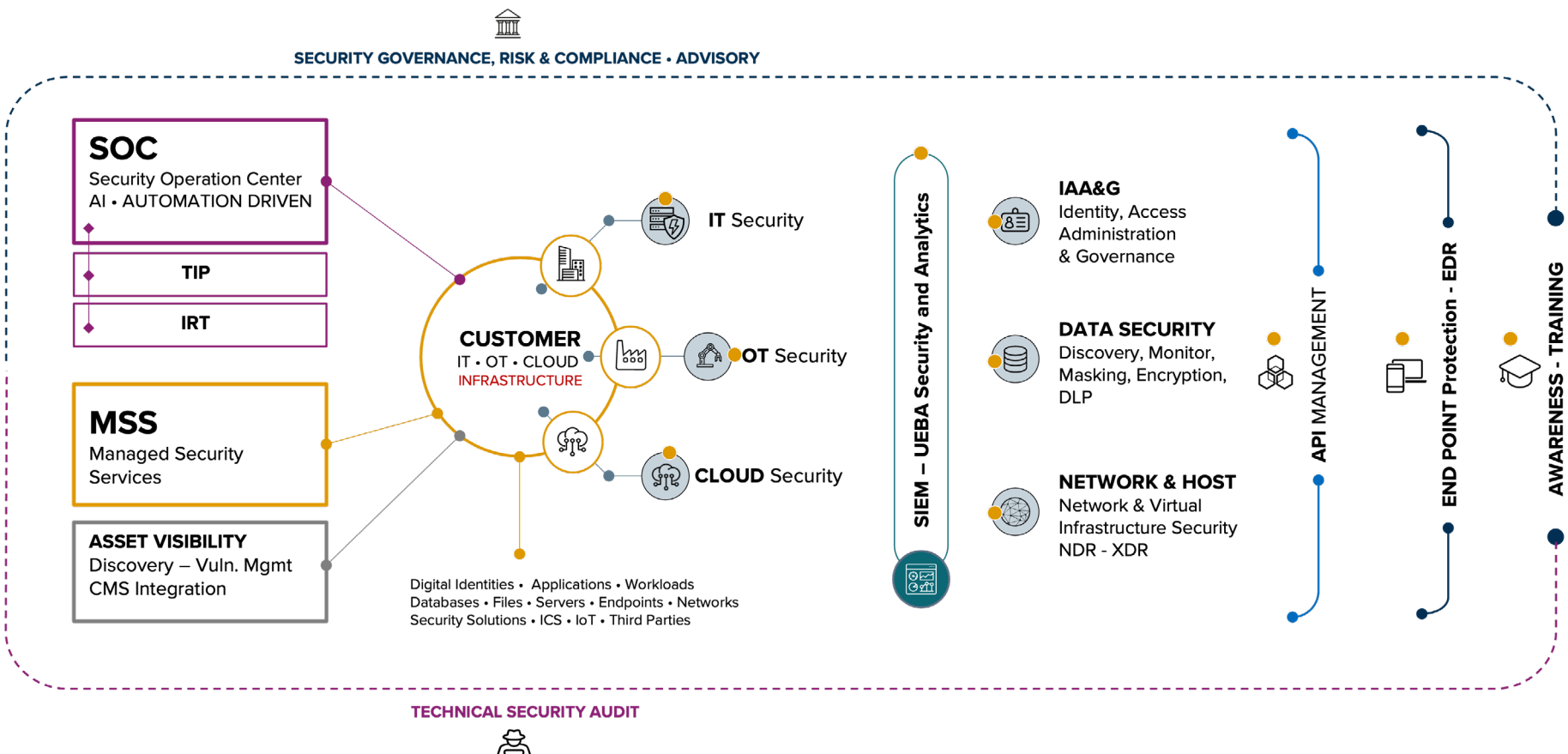
Soluzioni integrate multilivello offrono sicurezza a tutta l'organizzazione

In coerenza con il nostro approccio, abbiamo posizionato e sviluppato in un framework tecnologico consistente, le nostre competenze e le soluzioni nei vari domini della Cybersecurity ed i servizi sia di implementazione e supporto, sia gestiti attraverso il SOC.

Una architettura tecnologica completa ed organizzata in una struttura logica, per offrire soluzioni all'interno di un quadro integrato e trasversale.

Per i nostri clienti costruiamo e implementiamo soluzioni di Cybersecurity integrate e multilivello, così da supportare la fornitura sicura di nuovi servizi digitali, proteggendo al contempo l'accesso ad app e dati all'interno del mobile, dello IoT e dell'impresa cloud-connected. In questo modo aiutiamo le organizzazioni a:

- **migliorare** la capacità di visibilità, controllo e blocco della crescente superficie di minacce-cyber, raggiungendo una situazione di sicurezza adattiva e contestualizzata;
- **comprendere** il flusso di informazioni e migliorare le capacità di prevenire, individuare e reagire alle minacce-cyber;
- **salvaguardare** i propri dati per supportare il percorso della Digital Transformation.




Soluzioni integrate multilivello offrono sicurezza a tutta l'organizzazione

Soluzioni integrate multilivello offrono sicurezza a tutta l'organizzazione

L'architettura dei nostri servizi e soluzioni mette al centro il perimetro tecnologico del nostro cliente, che include l'infrastruttura IT, Operational Technology (OT) e le tecnologie Cloud. I nostri servizi e soluzioni ruotano attorno a questo nucleo, a partire da:

- i servizi di **Advisory e Governance Risk & Compliance**, per orchestrare la strategia di sicurezza del Cliente;
- i servizi di **Security Information and Event Management (SIEM)**, che includono attività legate ad Identity & Access Management (IAM), Data Security e Network & Host, nonché API Management ed Endpoin;
- i servizi gestiti, a partire da un Security Operations Center (SOC) fondato **sull'Intelligenza Artificiale e sull'automazione** e supportato da servizi avanzati di Threat Intelligence e Incident Response;
- i **Managed Security Services (MSS)** per la discovery e visibility di sicurezza degli asset, con i servizi di Vulnerability Management;
- i servizi volti ad aumentare le **competenze e l'awareness** in ambito Cybersecurity;
- i servizi di **Technical Security Audit**, che includono Vulnerability Assessment e Penetration Testing (VA / PT).

Focus On

## Il nostro Framework SOC e l'approccio Mesh

Il nostro SOC Framework è allineato agli standard di riferimento quali il **NIST Cybersecurity Framework**, e si ispira all'approccio componibile del **Mesh introdotto da Gartner**, teso a creare un ecosistema collaborativo di tool di sicurezza, operanti al di là del perimetro tradizionale, allineando allo stesso tempo i processi e l'organizzazione del SOC.

Secondo i principi del Mesh, nel framework architetturale del nostro SOC i **punti di controllo ed i presidi di sicurezza si avvicinano sempre di più agli asset da difendere**, e vengono integrati in una piattaforma centrale multi layered, che ospita le funzioni di analytics, automazione ed orchestrazione, e di dashboarding/reporting.

Soluzioni integrate multilivello offrono sicurezza a tutta l'organizzazione

# 05 Nuove tecnologie permettono di affrontare nuove minacce

La proliferazione di soluzioni tecnologiche e l'interconnessione di device e reti continuerà a caratterizzare il nostro sviluppo, creando purtroppo maggiori opportunità anche per i cyber attaccanti.

**Sei trend per la Cybersecurity al 2030:**

## **01** / MANCANZA DI COMPETENZE

La domanda del mercato del lavoro di professionisti in questo ambito continuerà ad aumentare, e c'è già una forte carenza di personale qualificato. L'ampliarsi di questa differenza potrebbe condurci a breve in una situazione in cui non ci sono abbastanza esperti per proteggere le infrastrutture critiche e rispondere agli attacchi. Per rispondere alla carenza di competenze in materia di sicurezza informatica occorrerà:

- una combinazione di strategie a breve e lungo termine, adottate e supportate da organizzazioni pubbliche e private, che comprende la promozione dell'istruzione e della formazione,
- lo sviluppo di programmi di apprendistato e tutoraggio, l'inclusione di competenze ed approcci diversi,
- l'utilizzo di strumenti di automazione e di intelligenza artificiale ed il mantenimento dei talenti esistenti.

## **02** / AUMENTO DELLO «SPESSORE» DELLE SOLUZIONI TECNOLOGICHE

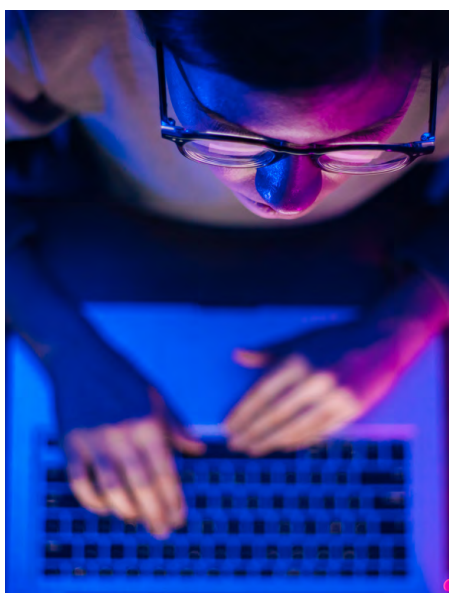
In linea con i progressi in campo di automazione e autonomia, le soluzioni tecnologiche saranno sempre più pervasive nelle nostre vite, professionali e personali. Questo sviluppo, verticale ed orizzontale, ha il controproducente effetto di aumentare il problema legato alla carenza di competenze professionali.

- Si renderà sempre più necessario bilanciare i progressi tecnologici con competenze di governo ed orchestrazione, delegando le attività più routinarie, senza tuttavia correre il rischio di sbilanciare l'equilibrio autonomia-controllo

## **03** / INFORMATION WARFARE

La crescente conduzione di operazioni di contrasto nello spazio cibernetico da parte degli Stati rappresenta una minaccia significativa per la sicurezza globale: gli hacker hanno ora risorse e competenze per lanciare attacchi sofisticati alle infrastrutture critiche e ai sistemi governativi; inoltre lo status giuridico di questo nuovo campo non è ancora chiaro. Sotto questa pressione, i governi di molti paesi hanno già emesso politiche operative di sicurezza nazionale per proteggere le loro infrastrutture informatiche, ma anche le imprese devono rafforzare le loro misure di sicurezza per ridurre i rischi di un eventuale attacco ad uno stato-nazione. Affrontare questa minaccia in continua evoluzione richiederà un approccio proattivo e sfaccettato che prevede:

- lo sviluppo di intelligence sulle minacce,
- l'implementazione di una strategia di difesa approfondita,
- lo svolgimento di regolari valutazioni della vulnerabilità,
- l'implementazione di controlli di accesso,
- lo sviluppo di piani di risposta agli incidenti e la promozione della collaborazione tra le parti interessate, pubbliche e private.



## **04** / ARTIFICIAL INTELLIGENCE

Il continuo sviluppo in campo AI ha messo a disposizione anche dei criminali informatici nuovi strumenti, che possono essere utilizzati per lanciare attacchi più sofisticati e complessi: l'intelligenza artificiale potrebbe essere utilizzata per generare email di phishing convincenti o per sfruttare le vulnerabilità nei sistemi informatici.
La risposta a questi nuovi attacchi, sviluppati tramite l'utilizzo di AI dai criminali informatici richiederà un approccio che lavora su più dimensioni:

- lo sviluppo di difese basate sull'intelligenza artificiale,
- l'implementazione di controlli di accesso,
- lo svolgimento di valutazioni della vulnerabilità regolari,
- la formazione dei dipendenti e la promozione della collaborazione,
- lo sviluppo di piani di risposta agli incidenti e l'aggiornamento regolare delle misure di sicurezza.

## **05** / INTERNET OF THINGS (IOT) AND CONNECTED DEVICES

L'aumento di intelligenza e connessione del nostro mondo fisico attraverso l'IoT, combinato con la diffusione della rete 5G, crea infatti perimetri di difesa sempre più fluidi introducendo nuove minacce-cyber, i cui impatti sulla società civile saranno sempre più rilevanti, come nei casi degli attacchi alle infrastrutture critiche che già osserviamo oggi. Affrontare le sfide della sicurezza informatica derivanti dalla diffusione dei dispositivi IoT richiede:

- una progettazione sicura, un'autenticazione forte, un controllo degli accessi,
- un monitoraggio continuo, segmentazione e isolamento,
- e una pianificazione della risposta agli incidenti.

## **06** / QUANTUM COMPUTING

I computer quantistici potrebbero potenzialmente violare molti dei metodi di crittografia attualmente utilizzati per proteggere i dati: mentre il calcolo quantistico diventa più diffuso, gli esperti di sicurezza informatica devono sviluppare nuovi metodi di crittografia in grado di resistere agli attacchi.

- Affrontare la possibile minaccia dell'informatica quantistica richiederà una combinazione di ricerca, sviluppo e pianificazione: adottando un approccio proattivo ed investendo in tecnologie resistenti ai quanti (Quantum-resistant cryptography, Quantum key distribution, Quantum-safe network infrastructure e Post-quantum security planning), le organizzazioni potranno proteggere meglio i propri dati e sistemi

**Per tutti i trend descritti, l'Europa ha fatto e sta facendo passi concreti verso una strategia volta ad aumentare la resilienza agli attacchi-cyber, concentrandosi sullo sviluppo di maggiore capacità e sul coordinamento dei processi di risposta e prevenzione.**

**Tuttavia, è indispensabile che anche le imprese rafforzino le loro misure di sicurezza per aumentare la resilienza complessiva del sistema.**

# 06 Una rete per innovare



## Engineering contribuisce attivamente alla ricerca in ambito cybersecurity, anche attraverso la partecipazione a iniziative in ambito Europeo e nazionale.

Promuoviamo l'innovazione: gestiamo progetti su tematiche emergenti, come il rapporto tra AI e Cybersecurity, la protezione delle infrastrutture essenziali, la sicurezza degli ambienti IoT, le tecniche di preservazione della privacy.

Offriamo un contributo concreto: i prototipi proposti dal nostro laboratorio sono basati su casi d'uso reali, elaborati sulle esigenze di diversi mercati tra cui energia, trasporti e sanità.

Focus On

# ENGINEERING È PLAYER EUROPEO NELLA CYBERSECURITY SIN DAL 2007.

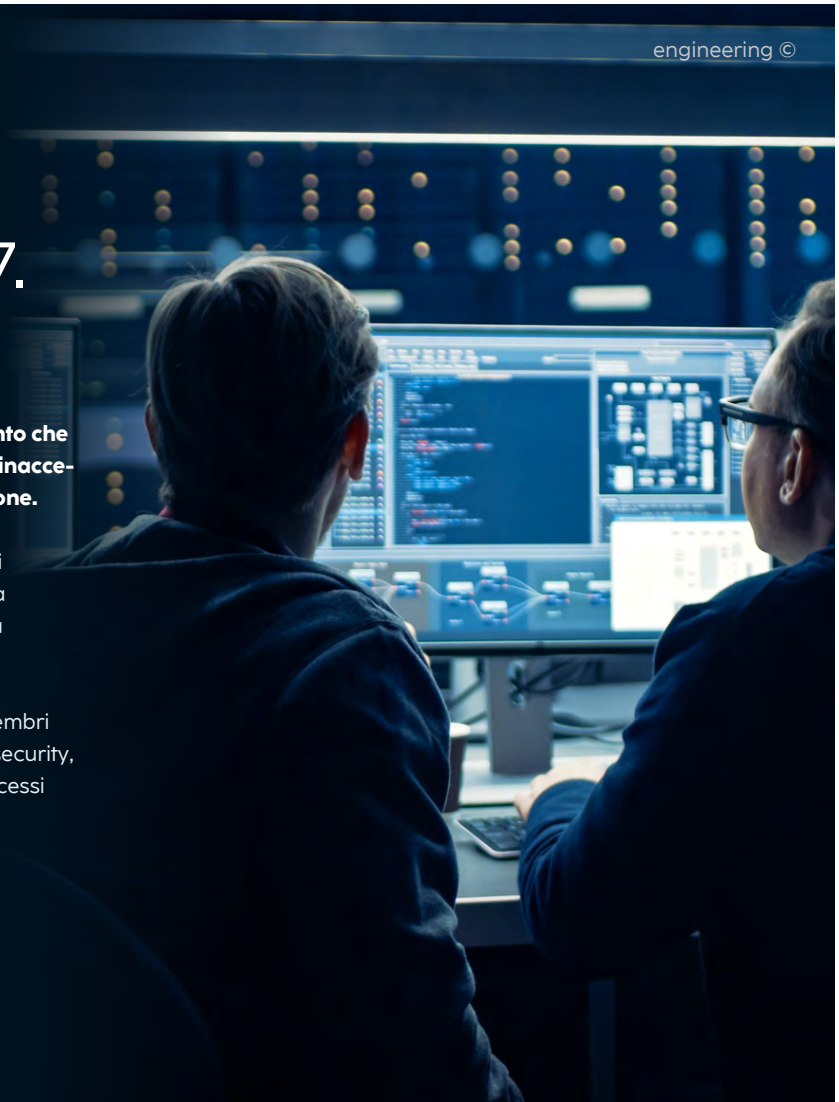
Nell'Organizzazione Europea per la Sicurezza (EOS) abbiamo promosso un approccio coordinato alla Cybersecurity con l'adozione di una strategia concertata. Insieme ai maggiori player della sicurezza in Europa, il nostro impegno nella promozione di un piano d'azione a livello europeo ha raggiunto un importante traguardo con la Cybersecurity private public partnership tra la Commissione Europea e i player industriali attraverso l'ECSO, l'European Cyber Security Organisation. In ECSO, Engineering guida il gruppo di lavoro per la ricerca relativa alla resilienza delle infrastrutture critiche da attacchi ed incidenti informatici.

Nel corso degli ultimi anni Engineering ha indirizzato le sue attività di ricerca nella Cybersecurity verso tre direzioni:

- **nuovi approcci per formare gli impiegati e i dipendenti pubblici a essere in grado di scoprire gli attacchi-cyber dannosi;**
- **valutazione integrata e continua del rischio cyber in contesti IT e OT, in particolare su infrastrutture critiche;**
- **determinazione delle priorità dell'investimento che siano basate sull'impatto economico delle minacce-cyber e sulla loro crescente contestualizzazione.**

Il Gruppo Engineering collabora con i principali enti di ricerca Nazionali (tra cui l'Osservatorio di Ricerca del Politecnico di Milano ed il Clusit) e con l'Agenzia Europea per la Cybersecurity, ENISA.

Di particolare importanza è la cooperazione dei membri di ENISA per dar vita ai Certificati europei di Cybersecurity, che saranno validi in tutta Europa per prodotti, processi e servizi.



RESEARCH PROJECT / SMART ENERGY & UTILITIES

## CyberSEAS – Cyber Securing Energy dAta Services:

Il drammatico aumento della superficie di attacco di una moderna rete elettrica rende fondamentali le soluzioni per proteggere i sistemi di trasmissione e distribuzione di energia elettrica da cyberattacchi in grado di interrompere la continuità operativa e di causare gravi incidenti di sicurezza. Il progetto, coordinato da Engineering, considera le sfide e i vincoli derivanti dalla presenza di fonti di energia rinnovabile decentralizzate e sistemi legacy nelle catene di approvvigionamento energetico.

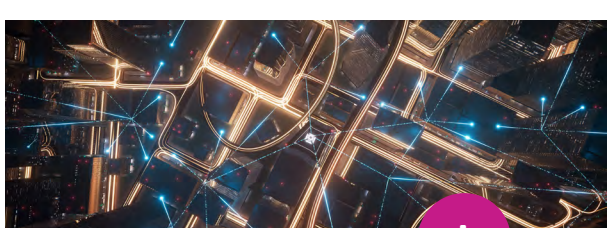
La soluzione prevede modelli innovativi di coinvolgimento dei produttori/distributori e dei consumatori in scenari di attacco complessi, offrendo un ecosistema aperto di soluzioni di sicurezza personalizzabili per prevenire, individuare e gestire i cyberattacks, incluso Social Engineering. Le soluzioni CyberSEAS sono validate attraverso campagne sperimentali su infrastrutture pilota in Italia, Croazia, Slovenia, Estonia, Romania e Finlandia.

RESEARCH PROJECT / DIGITAL INDUSTRY

## CERTIFY – aCtive sEcurity foR connecTed devIces liFecYcles:

In contesti IoT, ogni modifica alla sicurezza causata da una vulnerabilità o un aggiornamento non sicuro su un dispositivo la supply chain può mettere a rischio l'intero sistema. La gestione della sicurezza dell'IoT deve comprendere l'intero ciclo di vita dei prodotti e richiede il monitoraggio continuo e la certificazione per garantire un alto livello di sicurezza in linea con il recente Cybersecurity Act (CSA) europeo.

CERTIFY offre un approccio metodologico e soluzioni tecnologiche e organizzative per gestire la sicurezza dell'IoT, tra cui la progettazione, la valutazione e il monitoraggio continuo della sicurezza, la rilevazione, la mitigazione e la riconfigurazione tempestive, l'aggiornamento sicuro IoT Over-The-Air (OTA) e la condivisione continua di informazioni sulla sicurezza. Inoltre, CERTIFY consente agli attori dell'IoT di collaborare in modo decentralizzato e di proteggere le infrastrutture IoT da una vasta gamma di attacchi.



RESEARCH PROJECT / DIGITAL DEFENSE, AEROSPACE & HOMELAND SECURITY

## ENCRYPT – A scalable and practical privacy-preserving framework:

Le recenti tecnologie disponibili per facilitare l'elaborazione dei big data preservando la privacy (homomorphic encryption, differential privacy, secure multi-party computation, trusted execution environment, etc.) non sono ancora largamente adottate nella pratica.

ENCRYPT sviluppa un framework di tutela della privacy scalabile, pratico e adattabile a diversi contesti, validato nel settore sanitario per quanto riguarda lo scambio di informazioni di threat intelligence e nel settore finanziario per quanto concerne lo scambio transnazionale dei dati finanziari. Engineering è parte del progetto con una metodologia ed un prototipo che consente ai data controller una stima integrata e continua dei rischi di privacy e di cybersecurity in un approccio combinato alla protezione dei dati personali.

RESEARCH PROJECT / DIGITAL INDUSTRY

## KINAITICS – Cyber-kinetic attacks using Artificial Intelligence:

La diffusione dell'Intelligenza Artificiale apre le porte a nuovi tipi di attacchi, ma al contempo ha la potenzialità per allargare lo spettro di strumenti di cybersecurity classici per proteggersi da queste nuove minacce.

Sulla base di approcci specifici dedicati a quattro casi d'uso principali (finanza, CBRN, simulazioni al computer, salute), il progetto KINAITICS mira a produrre una serie di strumenti potenziati dall'intelligenza artificiale. Tali strumenti faranno progredire l'attuale stato dell'arte in attacco e difesa e saranno integrati in un quadro operativo in grado di simulare eventi informatici per formare esperti cyber e includere le loro reazioni nell'analisi. Nel progetto Engineering punta a evolvere i prototipi per la protezione da tecniche di ingegneria sociale e monitoraggio delle minacce informatiche, includendo nuove funzionalità basate sull'intelligenza artificiale.

RESEARCH PROJECT / E-HEALTH

## ERATOSTHENES – IoT Trust and Identity Management Framework:

Molte sono le recenti sfide poste dalle reti IoT: eterogeneità dei dispositivi, sicurezza dei sistemi, assenza di meccanismi comuni per la valutazione dell'affidabilità dei devices e di un framework di riferimento per la gestione di identità, privacy, formazione e protocolli di sicurezza degli ambienti IoT.

ERATOSTHENES supporta le organizzazioni nella previsione, monitoraggio e aggiornamento della sicurezza dei loro sistemi ICT, con particolare attenzione agli ambienti IoT. Sviluppa inoltre meccanismi inter-ledger per condividere e tenere traccia delle informazioni sulla sicurezza informatica in una rete di dispositivi IoT. Engineering guida l'integrazione del framework e partecipa alla validazione sui tre piloti in ambito automotive, healthcare e Industry 4.0 fornendo una soluzione per il rilevamento delle intrusioni in ambito IoT.

RESEARCH PROJECT / DIGITAL DEFENSE, AEROSPACE & HOMELAND SECURITY

## CitySCAPE – City-level Cyber-Secure Multimodal Transport Ecosystem:

Con la sua progressiva digitalizzazione, il settore dei trasporti è diventato sempre più interconnesso, con una sempre più spiccata centralizzazione dei servizi di controllo e gestione delle flotte e dei passeggeri. Tuttavia, questa architettura centralizzata aumenta la vulnerabilità agli attacchi informatici.

Il progetto CitySCAPE, di cui Engineering è partner, ha realizzato un toolkit modulare integrabile in qualsiasi sistema di trasporto multimodale per valutare l'impatto di un attacco in termini sia tecnici che finanziari, rilevare valori di dati di traffico sospetti e identificare minacce persistenti, combinare la conoscenza esterna e le attività osservate internamente per migliorare la prevedibilità degli attacchi zero-day. La soluzione è in fase di test su casi d'uso che coinvolgono applicazioni di biglietteria, frodi informatiche e dati sulla posizione nel sistema di trasporto regionale nelle municipalità di Tallinn (Estonia) e Genova (Italia).

# 07 KEY TAKEAWAYS
# Our Cybersecurity Fabric

key ta

**1**

La Cybersecurity è uno strumento della Digital Transformation: in quanto tale, è parte integrante della strategia di crescita aziendale.

**2**

Non riguarda solo la tecnologia: la Cybersecurity è una priorità ed una decisione di business a tutti gli effetti, e le persone ed i processi ne sono componenti essenziali.

**3**

È impossibile raggiungere un grado di sicurezza totale: è invece necessario comprendere profondamente i rischi per prioritizzare correttamente gli investimenti.

**4**

La valutazione del rischio è in continuo mutamento: è legata allo sviluppo del mercato e dell'azienda, così come all'evoluzione del panorama delle minacce Cyber. Pertanto deve aggiornarsi per conservare valore.

# keaways

## 5

Bisogna conoscere quello che si difende: ogni azienda ha il suo particolare sistema di riferimento, la propria interpretazione di asset critico (edifici, veicoli, computer e reti, ma anche trade secrets, piani di marketing e strategie di prezzo) e di accettabilità del rischio.

## 6

La prevenzione è l'altra faccia della difesa: lo studio dell'evoluzione delle minacce e l'analisi costante delle proprie vulnerabilità, anche dal punto di vista dell'attaccante, sono componenti costituenti nel piano di Cyber resilienza.

## 7

Identity first security, ovvero gestire in modo consapevole le identità digitali: in un mondo digitale senza perimetro, l'identificazione degli utenti e la corretta gestione dei loro permessi, in logica ZeroTrust, è la base su cui costruire ogni strategia di difesa.

## 8

Misurare è il primo passo per migliorare: la comprensione dei risultati conseguiti dalla cybersecurity e la condivisone delle evidenze con tutta l'azienda è necessaria per definire le azioni di miglioramento ed elevare le performance complessiva della sicurezza.

## 9

Il contesto normativo e gli standard sono degli alleati: i mandati di conformità, gli standard e le metodologie di riferimento migliorano la postura dei singoli e dell'ecosistema delle catene di valore.

## 10

Bisogna allenare la resilienza e saper reagire agli attacchi-cyber: verificare la tenuta dei piani di comunicazione, delle procedure di isolamento e del sistema di responsabilità sotteso per minimizzare i potenziali danni.

www.eng.it

Engineering Group

@LifeAtEngineering

@EngineeringSpa